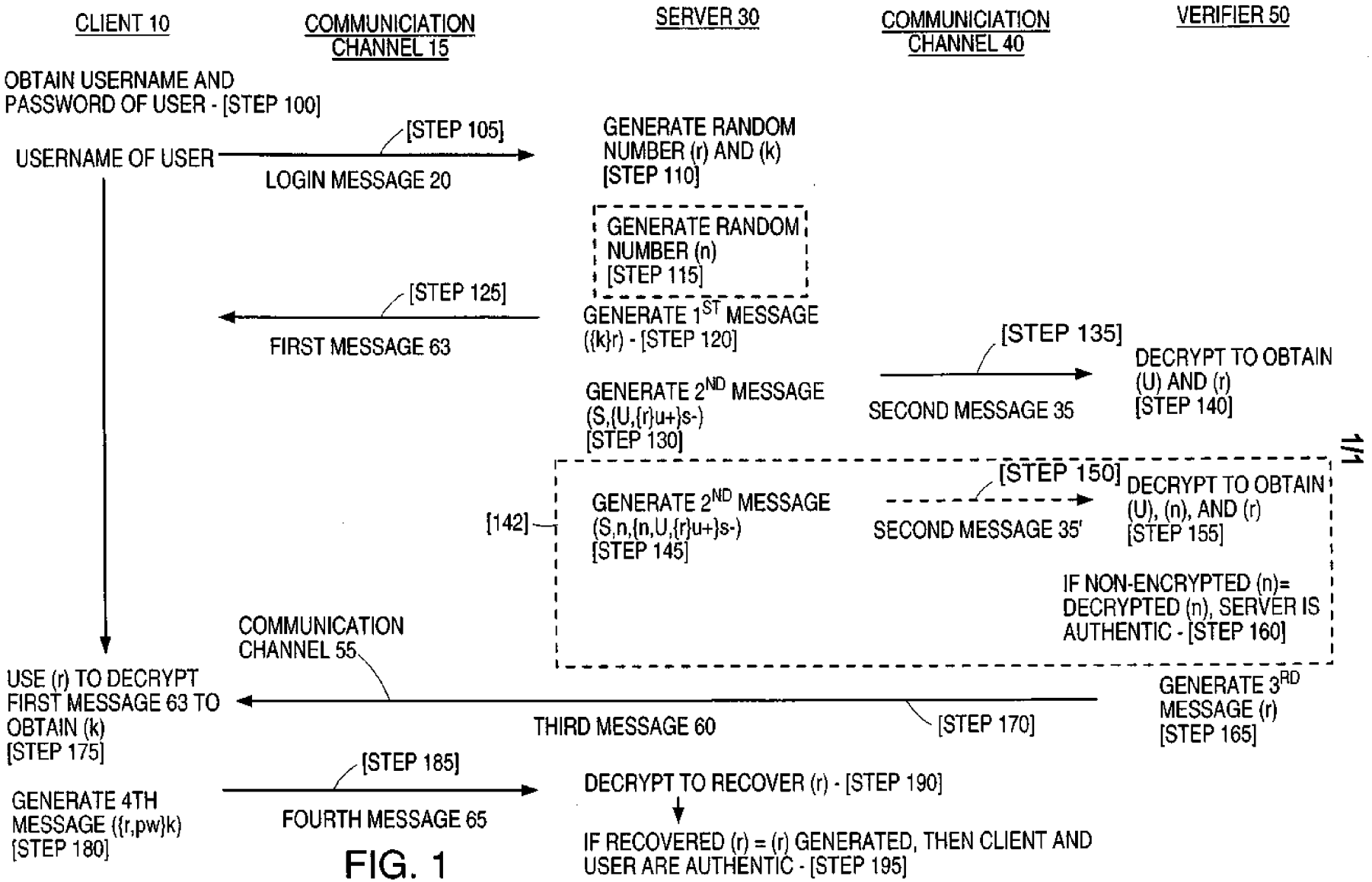
CLIENT 10
COMMUNICIATION CHANNEL 15
SERVER 30
COMMUNICIATION CHANNEL 40
VERIFIER 50
OBTAIN USERNAME AND PASSWORD OF USER - [STEP 100]
[STEP 105]
USERNAME OF USER
LOGIN MESSAGE 20
GENERATE RANDOM NUMBER (r) AND (k) [STEP 110]
GENERATE RANDOM NUMBER (n) [STEP 115]
[STEP 125]
FIRST MESSAGE 63
GENERATE 1ST MESSAGE ({k}r) - [STEP 120]
[STEP 135]
SECOND MESSAGE 35
DECRYPT TO OBTAIN (U) AND (r) [STEP 140]
GENERATE 2ND MESSAGE (S,{U,{r}u+}s-) [STEP 130]
[142]
GENERATE 2ND MESSAGE (S,n,{n,U,{r}u+}s-) [STEP 145]
[STEP 150]
SECOND MESSAGE 35'
DECRYPT TO OBTAIN (U), (n), AND (r) [STEP 155]
IF NON-ENCRYPTED (n)= DECRYPTED (n), SERVER IS AUTHENTIC - [STEP 160]
COMMUNICATION CHANNEL 55
USE (r) TO DECRYPT FIRST MESSAGE 63 TO OBTAIN (k) [STEP 175]
THIRD MESSAGE 60
[STEP 170]
GENERATE 3RD MESSAGE (r) [STEP 165]
[STEP 185]
GENERATE 4TH MESSAGE ({r,pw}k) [STEP 180]
FOURTH MESSAGE 65
DECRYPT TO RECOVER (r) - [STEP 190]
IF RECOVERED (r) = (r) GENERATED, THEN CLIENT AND USER ARE AUTHENTIC - [STEP 195]

FIG. 1

1/1